REMARKS

The Applicants and the undersigned thank Examiner Jackson for her careful review of this application. Claims 1, 2, 5, and 7-25 have been rejected. Upon entry of this amendment, Claim 5 has been cancelled and Claims 1-4, and 6-25 are pending in this application.

The independent claims are Claims 1, 3, 6, 12, 13, 16, 19, 21, and 25. Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Allowed Dependent Claims 3 and 6 Re-Written in Independent Form

The Applicants appreciate the indication of allowable subject matter in previous dependent Claims 3-4 and 6. The Applicants have rewritten dependent Claim 3 and Claim 6 as independent claims such that they have all of the limitations of their previous independent claims. It is believed that Claims 3, 4 (by its dependency on Claim 3), and 6 are allowable over the prior art. Consideration and an indication from the Examiner that these claims are allowable over the prior art are respectfully requested.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected Claims 1-2, 5, and 7-25 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,510,523 to Perlman (hereinafter the "Perlman" reference). The Applicants respectfully offer remarks to traverse these pending rejections.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Perlman reference fails to describe, teach, or suggest the combination of (1) completing a vulnerability assessment comprising (2) a scan of the workstation to identify at least one of (a) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (b) evidence of a compromise; (3) generating workstation security credentials based on the vulnerability assessment, (4) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; (5) comparing the workstation

should be granted access to the network service; and (6) authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, otherwise denying access to the network service by the workstation, as recited in amended Claim 1.

The Perlman Reference

The Perlman reference describes a limited security system 100 for restricting user access privileges through an untrusted terminal 110 connected to a network. Limited security system 100 includes an untrusted terminal 110, credentials server 120, a Remote Terminal "A" 130, and a Remote Terminal "B" 140 connected by network 150. See Figure 1 of the Perlman reference illustrated below. See Column 4, lines 10-17 of the Perlman reference.

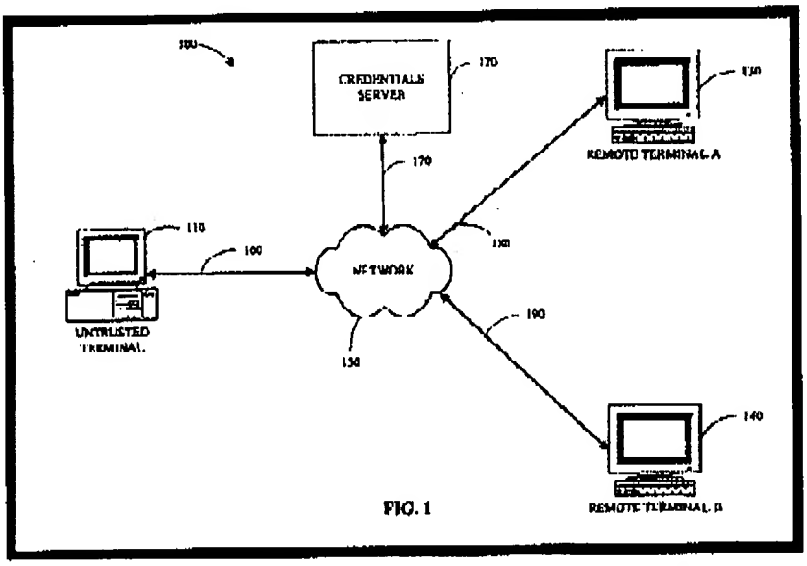


FIG. 1

Untrusted terminal 110 is a device capable of communicating with network 150 (e.g., via a modem or other communications device). Untrusted terminal 110 may have Internet access capabilities to communicate with remote terminals worldwide. Thus, if a user is vacationing in Australia, for example, they would be able to connect with their company server in Spokane, Washington via untrusted terminal 110. In addition, untrusted terminal 110 may include software that allows the user to locate and access information on remote terminals connected to network 150. One type of software

suitable for this purpose is a web browser, such as Netscape Navigator, which enables untrusted terminal 110 to connect to a server having a unique uniform resource locator (URL).

The Perlman reference describes the credentials server 120 as a device (e.g., server) connected to network 150 that is capable of generating credentials (e.g., a private key and a public key certificate) trusted by one or more remote terminals. Credentials server 120 issues credentials to a user to permit privileged operations. These credentials typically include public key certificates. However, credentials server 120 can issue various kinds of credentials, depending on the requests from untrusted terminal 110. See Column 4, lines 38-46 of the Perlman reference.

Remote Terminal A 130 and Remote Terminal B 140 are computers connected to network 150 that can send data to and receive data from untrusted terminal 110. One remote terminal can be the user's company server and the other can be the server of a financial institution. Each terminal is capable of performing privileged operations, such as providing remote access to files and other data that is stored in the terminals 130 and 140. See Column 4, lines 53-58 of the Perlman reference.

As part of establishing the secure communications channel between the untrusted terminal 110 and the remote terminals 130, 140, the credentials server 120 must identify the untrusted terminal 110 as "untrusted." The Perlman reference explains that this identification can be established using a variety of mechanisms. For example, the credentials server 120 may identify a terminal 110 as trusted or untrusted based on the network address of the terminal 110. See Perlman reference, column 5, lines 3-8.

In addition, a firewall connected to the credentials server 120 may insert a flag into a data packet of a request to establish a secure communications channel indicating that the terminal 110 generating the request should not be trusted (i.e., because the request originated outside of the credentials server network). Alternatively, a terminal 110 may prove that it is trusted by demonstrating knowledge of a secret or a private key whose public key has been certified as belonging to a trusted workstation. Moreover, if a terminal 110 simply cannot prove it should be trusted, the credential server 120 can identify the terminal 110 as untrusted when establishing the secure communication channel. See Perlman reference, column 5, lines 9-20.

The Perlman Vulnerability Assessment (1) does not include a scan that can find evidence of a compromise and (2) the Assessment is not connected to allowing the workstation to access the secure network

The Examiner states in paragraph number 3 of the Final Office Action mailed on January 14, 2005 that it is inherent that the Perlman reference completes a vulnerability assessment of the workstation. The Examiner believes that the Perlman reference completes a vulnerability assessment because Perlman discloses that the credential server generates credentials and issues these credentials to perform privileged operations on the remote terminal.

These alleged facts made by the Examiner do not reasonably support that the Perlman reference inherently (a) performs a vulnerability assessment comprising a scan of the workstation to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise; (b) comparing the workstation security credentials to a workstation security policy to determine whether the workstation should be granted access to the network service; and (c) authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy.

The Examiner has provide not basis in fact or technical reasoning to reasonably support that the Perlman reference provides a vulnerability assessment that is identical to that of the Applicants' as claimed and that the vulnerability assessment is used to generate workstation security credentials that are used to determine whether a workstation should be granted access to the network. The Applicants remind the Examiner that MPEP § 2112, subsection IV, second paragraph states the following:

> "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." Ex parte Levy, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990).

The Examiner alleges that the production of "credentials" alone in the Perlman reference means that it is inherent that the Perlman reference completes a vulnerability assessment that is identical to Applicants' claimed technology. However, the Applicants respectfully disagree. The Perlman reference is only concerned with if it can identify a terminal based on the identity of the user or based on whether a terminal knows a secret or a private key. See the Perlman reference, column 4, lines 42-46. If the Perlman reference cannot identify a remote terminal, it simply characterizes the remote terminal as "untrusted" and the Perlman reference then limits the amount of access that the "untrusted" terminal can have to the computer network.

Meanwhile, the Applicants' invention as recited in amended independent Claim 1 performs a vulnerability assessment comprising a scan of the workstation to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise. The Applicants submit that the Perlman does not provide any teaching of such a vulnerability assessment with this level of detail as now recited in amended independent Claim 1.

The Applicants also submit that its claimed vulnerability assessment is connected with the security credentials that are produced. They are connected meaning that the security credentials are produced based upon the completion of the vulnerability assessment. Because the Perlman reference does not conduct a vulnerability assessment, its credentials are not connected or related to any vulnerability assessment.

In light of the differences between Claim 1 and the Perlman reference, one of ordinary skill in the art recognizes that this prior art reference, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

Independent Claim 12

The rejection of Claim 12 is respectfully traversed. It is respectfully submitted that the Perlman reference, fails to describe, teach, or suggest the combination of (1) a local workstation assessment service, operative on the workstation, for (2) generating workstation security credentials by (3) completing a vulnerability assessment of the

workstation comprising a scan to identify at least one of (i) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (ii) evidence of a compromise, (4) the workstation security credentials comprising (a) one of integrity information describing whether the workstation has been compromised, and (b) security posture information describing the workstation's potential for compromise; and (5) a workstation security policy, operative on the workstation, for defining security policy requirements for secure operations by the workstation; (6) the local workstation assessment service further operative for comparing the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service, (7) the local workstation assessment service further operative to authorize access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, as recited in amended Claim 12.

As noted above with respect to independent Claim 1, the Perlman reference does not provide a teaching of vulnerability assessment of the workstation comprising a scan to identify at least one of (i) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (ii) evidence of a compromise.

In light of the differences between Claim 12 and the Perlman reference, one of ordinary skill in the art recognizes that the Perlman reference, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 12. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 13

The rejection of Claim 13 is respectfully traversed. It is respectfully submitted that the Perlman reference, fails to describe, teach, or suggest the combination of (1) a local workstation assessment service, operative on the workstation, (2) for generating workstation security credentials by (3) completing a vulnerability assessment comprising (4) a scan of the workstation to identify at least one of (5) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (6) evidence of a compromise, the workstation security credentials comprising one of (7)

integrity information describing whether the workstation has been compromised, and (8) security posture information describing the workstation's potential for compromise; and (9) a network service, operative on the network server, for (10) determining whether the workstation should be granted access to a software service of the network service in response to receiving the workstation security credentials via the computer network, as recited in amended Claim 13.

As noted above with respect to independent Claim 1, the Perlman reference does not provide a teaching of vulnerability assessment of the workstation comprising a scan to identify at least one of (i) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (ii) evidence of a compromise.

In light of the differences between Claim 13 and the Perlman reference, one of ordinary skill in the art recognizes that the Perlman reference, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 13. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 16

The rejection of Claim 16 is respectfully traversed. It is respectfully submitted that the Perlman reference, fails to describe, teach, or suggest the combination of a (1) network service operative to generate workstation security credentials by (2) completing a vulnerability assessment comprising a (3) scan of the workstation to identify at least one of (4) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (5) evidence of a compromise, the workstation security credentials comprising (6) one of integrity information describing whether the workstation has been compromised, and (7) security posture information describing the workstation's potential for compromise; (8) the network service further operative to determine whether the workstation should be granted access to a software service of the network based on the workstation security credentials, as recited in amended Claim 16.

As noted above with respect to independent Claim 1, the Perlman reference does not provide a teaching of vulnerability assessment of the workstation comprising a scan

to identify at least one of (i) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (ii) evidence of a compromise.

In light of the differences between Claim 16 and the Perlman reference, one of ordinary skill in the art recognizes that the Perlman reference, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 16. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 19

The rejection of Claim 19 is respectfully traversed. It is respectfully submitted that the Perlman reference, fails to describe, teach, or suggest the combination of (1) issuing a request for a log in page to a network server from a browser operating on the workstation; (2) transmitting the log-in page and an authentication plug-in from the network server to the workstation via the computer network, the authentication plug-in installable within the browser and operative to generate workstation security credentials by (3) completing a vulnerability assessment comprising a (4) scan of the workstation to identify at least one of (5) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (6) evidence of a compromise, (7) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; (8) transmitting the workstation security credentials from the authentication plug-in to the network server via the computer network; and (9) determining at a CGI script operating on the network server whether the workstation should be granted access to a software service of the network based on the workstation security credentials, as recited in amended Claim 19.

As noted above with respect to independent Claim 1, the Perlman reference does not provide a teaching of vulnerability assessment of the workstation comprising a scan to identify at least one of (i) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (ii) evidence of a compromise.

In light of the differences between Claim 19 and the Perlman reference, one of ordinary skill in the art recognizes that the Perlman reference, alone or in combination,

cannot anticipate or render obvious the recitations as set forth in amended independent Claim 19. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 21

The rejection of Claim 21 is respectfully traversed. It is respectfully submitted that the Perlman reference, fails to describe, teach, or suggest the combination of a (1) network assessment service operating on a network workstation assessment server on the computer network, the network assessment service operative to (2) generate workstation security credentials prior to receiving user credentials by (3) completing a vulnerability assessment comprising a (4) scan of the workstation via the computer network to identify at least one of (5) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (6) evidence of a compromise, (7) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, (8) the network service, responsive to receiving the workstation security credentials from the network assessment service via the computer, operative to determine whether (9) the workstation should be granted access to a software service of the network based on the workstation security credentials and the user credentials, as recited in amended Claim 21.

As noted above with respect to independent Claim 1, the Perlman reference does not provide a teaching of vulnerability assessment of the workstation comprising a scan to identify at least one of (i) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (ii) evidence of a compromise.

In light of the differences between Claim 21 and the Perlman reference mentioned above, one of ordinary skill in the art recognizes that the Perlman reference, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 21. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 25

The rejection of Claim 25 is respectfully traversed. It is respectfully submitted that the Perlman reference, fails to describe, teach, or suggest the combination of (1) issuing a request for a log-in page to a network server from a browser operating on the workstation; (2) transmitting the log-in page, (3) an authentication plug-in, and a (4) workstation policy from the network server to the workstation via the computer network, (5) the authentication plug-in installable within the browser and operative to generate workstation security credentials by (6) completing a vulnerability assessment comprising (7) a scan of the workstation to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (8) evidence of a compromise, (9) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; (10) comparing the workstation security credentials to the workstation policy on the workstation to determine whether the workstation should be granted access to a software service of the network; and (11) receiving user credentials if the workstation is granted access to the software service of the network, as recited in amended Claim 25.

As noted above with respect to independent Claim 1, the Perlman reference does not provide a teaching of vulnerability assessment of the workstation comprising a scan to identify at least one of (i) security vulnerabilities that would compromise the secure operation of the workstation on the computer network and (ii) evidence of a compromise.

In light of the differences between Claim 25 and the Perlman reference mentioned above, one of ordinary skill in the art recognizes that the Perlman reference, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 25. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2, 4, 7-11, 14-15, 17-18, 20, and 22-24

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references.

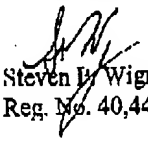
The Applicants also respectfully submit that the recitations of dependent Claims 2, 4, 7-11, 14-15, 17-18, 20, and 22 24 are of patentable significance. Accordingly, reconsideration and withdrawal of the rejections of the dependent claims are respectfully requested.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on January 14, 2005. The Applicants and the undersigned thank Examiner Jackson for the consideration of these remarks. The Applicants have submitted remarks to traverse the rejections of Claims 1-25. The Applicants respectfully submit that the present application is in condition for allowance. Such Action is hereby courteously solicited.

If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.2884.

Respectfully submitted,



Steven D. Wigmore
Reg. No. 40,447

King & Spalding LLP
45th Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404.572.4600
K&S Docket: 05456-105004